UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

GOOGLE LLC, *Plaintiff*, v. DMITRY STAROVIKOV; ALEXANDER FILIPPOV; and Does 1-15, *Defendants*.	Civil Action No. **FILED UNDER SEAL**

DECLARATION OF ELIZABETH A. BISBEE

I. Introduction and Witness Background

1. My name is Elizabeth (Beth) A. Bisbee. I am the head of U.S. investigations for Chainalysis Inc., a blockchain analytics and forensic investigative firm.

2. Prior to joining Chainalysis in January 2021, I was the Drug Enforcement Agency's national subject matter expert for virtual currency investigations, practices, and policies. In that role, I served as the Agency's lead expert witness for virtual currency and was involved in over 400 virtual currency investigations, including work on covert operations, blockchain analysis, suspect interviews, seizure of cryptocurrency, and trial preparation and testimony. I developed the Agency's training curriculum related to virtual currency and blockchain analysis, and I have taught numerous classes on virtual currency and virtual currency investigations. My work has been published in the Department of Justice's Journal of Federal Law and Practice.

3. This declaration is based on my personal knowledge. If called as a witness I could and would competently testify to the matters stated herein.

II. Overview of Chainalysis and Cryptocurrency

4. Chainalysis is a privately-owned software company that provides blockchain data solutions and supports the investigative, compliance, and risk management needs of government agencies and private companies. Chainalysis's Investigations and Special Programs ("ISP") group is a team of world-class investigators who provide unparalleled blockchain forensics support and

cryptocurrency transaction tracing using specialized expertise in proprietary Chainalysis software, open-source data research, and other investigative techniques. These methods have proven reliable in identifying and understanding the persons and entities responsible for cryptocurrency transactions.

5. For example, Chainalysis has recently assisted in a number of high-profile federal law enforcement actions involving cryptocurrency, including the takedown of two terrorism financing campaigns led by al-Qaeda and al-Qassam Brigades[1]; the seizure of $1 billion in cryptocurrency connected to the infamous dark web market, Silk Road[2]; the forfeiture of 280 cryptocurrency addresses associated with North Korean hackers[3]; and the sanctioning by the U.S. Treasury Department of Russian cryptocurrency exchange, Suex[4].

6. On behalf of Google, King & Spalding LLP ("Counsel") retained Chainalysis to use its specialized cryptocurrency investigative expertise to investigate the Glupteba botnet and enterprise.

---

[1] *Department of Justice Announces Takedown of Two Terrorism Financing Campaigns with Help from Blockchain Analysis*, CHAINALYSIS INSIGHTS BLOG (Aug. 13, 2020), https://blog.chainalysis.com/reports/cryptocurrency-terrorism-financing-al-qaeda-al-qassam-brigades-bitcointransfer.

[2] *US Government Agencies Seize More Than $1 Billion in Cryptocurrency Connected to Infamous Darknet Market Silk Road*, CHAINALYSIS INSIGHTS BLOG (Nov. 5, 2020), https://blog.chainalysis.com/reports/silk-road-doj-seizure-november-2020.

[3] *Justice Department Demands Forfeiture of 280 Cryptocurrency Addresses Associated with North Korea Exchange Hackers*, CHAINALYSIS INSIGHTS BLOG (Aug. 28, 2020), https://blog.chainalysis.com/reports/lazarus-group-north-korea-doj-complaint-august-2020.

[4] *OFAC Sanctions Russian Cryptocurrency OTC Suex that Received Over $160 million from Ransomware Attackers, Scammers, and Darknet Markets*, CHAINALYSIS INSIGHTS BLOG (Sept. 21, 2021), https://blog.chainalysis.com/reports/ofac-sanction-suex-september-2021.

7. Cryptocurrency is a type of virtual currency that may be used as a substitute for fiat currency. Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Examples of cryptocurrencies include Bitcoin, Ethereum, Dogecoin, and Monero.

8. One of the defining characteristics of cryptocurrency is that it is decentralized and peer-to-peer network-based. This means that no single person or entity has control. Rather, all users of a cryptocurrency retain collective control, and users may exchange cryptocurrency between themselves directly without the involvement of a central authority.

9. Payments or transfers of value made with most cryptocurrency are recorded on public distributed ledgers, often referred to as a "blockchain." The blockchain is run by the decentralized network for each cryptocurrency and contains the historical records of every transaction ("blocks"). Even though the public addresses of those engaging in cryptocurrency transactions are recorded on a blockchain, the identities of the individuals or entities behind the public addresses are not recorded on these ledgers. This is why cryptocurrency transactions are sometimes described as "pseudonymous," or partially anonymous. Thus, cryptocurrency allows users to transfer funds more anonymously[5] than would be possible through traditional banking and financial systems.

[5] Some cryptocurrencies, referred to as "privacy coins," have additional layers of anonymity. For example, Monero is a decentralized public distributed ledger with privacy-enhancing technologies that obfuscate transaction details, such as value

10. There are several ways for users to acquire cryptocurrency. The most straightforward way is directly from other users. Another common way to acquire cryptocurrency is through a cryptocurrency exchange, an online company that enables individuals to purchase or sell cryptocurrencies in exchange for fiat currencies or other cryptocurrencies. Coinbase is one example of a popular cryptocurrency exchange.

11. Users can also acquire cryptocurrency by "mining," which involves an individual using their computer's computing power to solve a complicated "proof of work" algorithm and then verifying and recording payments on the blockchain by operating a node (the computer) on the peer-to-peer network. The node validates transactions and broadcasts to other connected nodes within the network. Transaction fees are used to incentivize the miners in selecting transactions; typically, the higher the transaction fees, the more quickly the transactions are confirmed. Miners are rewarded for being the first to successfully complete this computational task by receiving newly created units of cryptocurrency and the fees associated with the transactions.

12. Cryptocurrencies are stored in a virtual account called a "wallet." Wallets are software programs. Wallets interface with a cryptocurrency's blockchain and store the public and private "keys" used to send and receive cryptocurrency. A public key, or "address," is akin to a bank account number, and a

---

being transferred and the cryptocurrency address (or addresses). These privacy features add additional layers of anonymity compared to Bitcoin.

private key is akin to a PIN or password that allows a user the ability to access and transfer value associated with the public address and the private key. To conduct transactions on a blockchain, an individual must use the public address and the corresponding private key. A wallet is a collection of private keys that correspond to addresses.

13. A transaction consists of at least three things: an input, output, and the amount. The input is the public address from which value is sent. The output is the public address receiving the value. The value being sent cannot be divided if the value being sent is more than the output should receive. When this occurs, the wallet software generates a "change address" to send the remainder value to as another output. This is similar to buying a $5 coffee with a $20 bill. The $20 bill cannot be divided into quarters to pay for the $5 coffee. Instead, change is provided to the purchaser. A collection of cryptocurrency addresses that co-spend (*i.e.*, addresses that are observed to be on the same input side of a transaction) are highly likely to be controlled by the same individual. This association of addresses is often referred to as "grouping" or "cluster."

14. Chainalysis collects and catalogues data associated with particular cryptocurrency transactions and, where possible, uses that data to identify or assist third parties in identifying the entities behind the transactions.

III. How the Glupteba Botnet Utilizes Blockchain

15. In September 2021, Chainalysis was retained by Counsel to conduct research and analysis involving the Glupteba botnet, a network of hundreds of

thousands of infected computers ("bots") under the control of cybercriminals based in Russia (the "Glupteba Enterprise" or the "Enterprise"). The bots are all connected to "command and control" servers ("C2 servers"), which are used by the Glupteba Enterprise to relay instructions to the bots (*e.g.*, "steal credentials" or "mine cryptocurrency").

16. Chainalysis was provided with Google's analysis of Glupteba's malicious software ("malware"), the Glupteba botnet, and the Glupteba Enterprise. Google identified three Bitcoin addresses believed to be hard-coded into Glupteba's code to communicate with the C2 servers.

17. Compared to a conventional botnet, the Glupteba botnet is uniquely dangerous because of the way it uses the Bitcoin blockchain to evade disruption. A conventional botnet encodes as its C2 server a particular domain address (*e.g.*, gfixprice.xyz), which the bots access to receive their instructions. If authorities or victims are able to shut down that domain address, the infected device can no longer receive its instructions and can therefore no longer be controlled by the Enterprise. This is a difficult task in and of itself. First, the C2 servers would have to be disabled by the domain registrar which sold the domain to the threat actors. Second, the hosting provider of the Enterprise's content delivery network ("CDN") servers must lock them out of those servers. Finally, any service providers that route traffic to the CDN servers for performance and resilience must disable the routing of traffic tied to the C2 servers.

18. For that reason, conventional botnet operators generally own several "disposable" domains—often created en masse by domain generation algorithms—as a defense against law enforcement action to disrupt the botnet. This is not a particularly efficient or resilient method to maintain a botnet because the malware-infected machines with the old C2 server domains can no longer serve their purpose. Unlike conventional botnets, the Glupteba botnet does not rely on hard-coded domains for the bots to communicate with the C2 servers. Instead, Glupteba malware is hard coded to "search" the public Bitcoin blockchain for specific transactions that the Glupteba Enterprise has encrypted with information on the C2 servers. In doing so, the Enterprise can continue to communicate instructions to the bots comprising the botnet even when its current C2 domains are disrupted.

19. Instead of being coded to visit a particular website in order to retrieve their instructions, the infected computers are programmed to search a public repository of Bitcoin transactions for those transactions related to specific public keys and wallets. The malware performs this by utilizing a transaction-specific function on the Bitcoin blockchain known as "OP_Return." An OP_Return is a Bitcoin "transaction" with no monetary value behind it. Rather, it is either sent as a simple standalone, valueless data transmission or it accompanies a transaction where funds are exchanged. Put simply, an OP_Return is used to communicate messages or data from one Bitcoin address to another. One could think of this as the Bitcoin version of a check memo line or the payment note in Google Pay (*e.g.*, for

dog walking), although, as explained, it need not accompany any transmission of value at all.

20. If one of the Glupteba botnet's C2 servers goes offline, the infected devices query the blockchain for an OP_Return message from one of three specified Bitcoin addresses sent by the Glupteba Enterprise. That OP_Return contains the address of the new C2 server in an encrypted code that Glupteba malware is programmed to decrypt. Therefore, unlike with conventional botnets, disrupting the Glupteba botnet for any meaningful length of time requires the blockchain-based infrastructure to be neutralized.

IV. Chainalysis's Investigation into the Glupteba Botnet

a. OP_Return Transactions Observed

21. Chainalysis was provided with three Bitcoin addresses—15y7dskU5TqNHXRtu5wzBpXdY5mT4RZNC6 (the "15y7" address), 1CgPCp3E9399ZFodMnTSSvaf5TpGiym2N1 (the "1CgPC" address), and 1CUhaTe3AiP9Tdr4B6wedoe9vNsymLiD97 (the "1CUha" address)—that Google identified in 2021 as hard-coded into Glupteba's malware. By analyzing the public blockchain between September 8, 2021 and October 25, 2021, Chainalysis determined the dates that these addresses were active and the number of OP_Return transactions sent from each address, as shown below.

Glupteba Bitcoin Addresses Overview

Bitcoin Address	Date Range Active	OP_Returns Sent
15y7d Address	June 17, 2019 to May 13, 2020	8
1CgPC Address	April 8, 2020 to October 19, 2021	6
1CUha Address	October 13, 2021	1

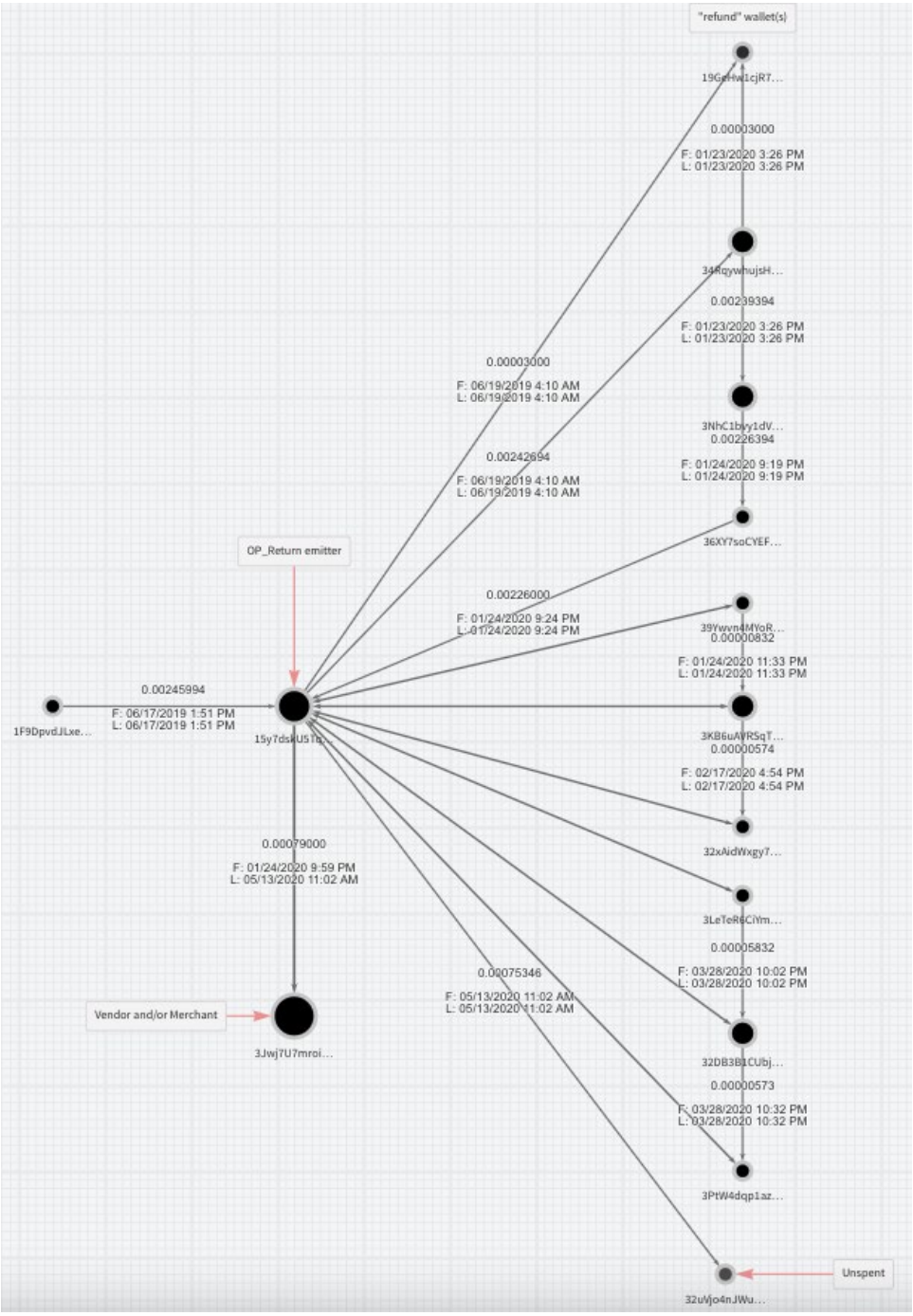
22. The 15y7d address was active between June 17, 2019 and May 13, 2020. During that time, the 15y7d address was observed sending a total of 24 small-value transfers, with eight accompanying OP_Returns. The initial funding of the 15y7d address appears to have been from a June 17, 2019 output in the amount of .00245994 Bitcoin[6] from a cluster identified by Chainanalysis. The initial funding was then used to fund the transactions with OP_Returns.

23. Beginning on June 19, 2019, the first OP_Return was sent in a transaction in the amount of .00242694 Bitcoin with three outputs: (1) the OP_Return, (2) a Bitcoin address that received most of the funds, and (3) another address receiving partial funds. This same transaction structure was repeated seven times between January 24, 2020 and May 13, 2020. Of note, address 15y7d had seven outputs containing OP_Return messages and partial funds spent to address 3Jwj7U7mroikfQ5uZ9iUV8frnLjNPfZ7nZ. Chainalysis designated with a high degree of confidence that address 3Jwj7 is a vendor and/or merchant. After six of these transactions, the funds were returned, or refunded, to the 15y7d address.

[6] On June 17, 2019, Bitcoin closed at $9,320.35, meaning that the value of this transaction in U.S. Dollars would have been approximately $22.92. *See* Bitcoin-USD, YAHOO! FINANCE, https://finance.yahoo.com/quote/BTC-USD/history/.

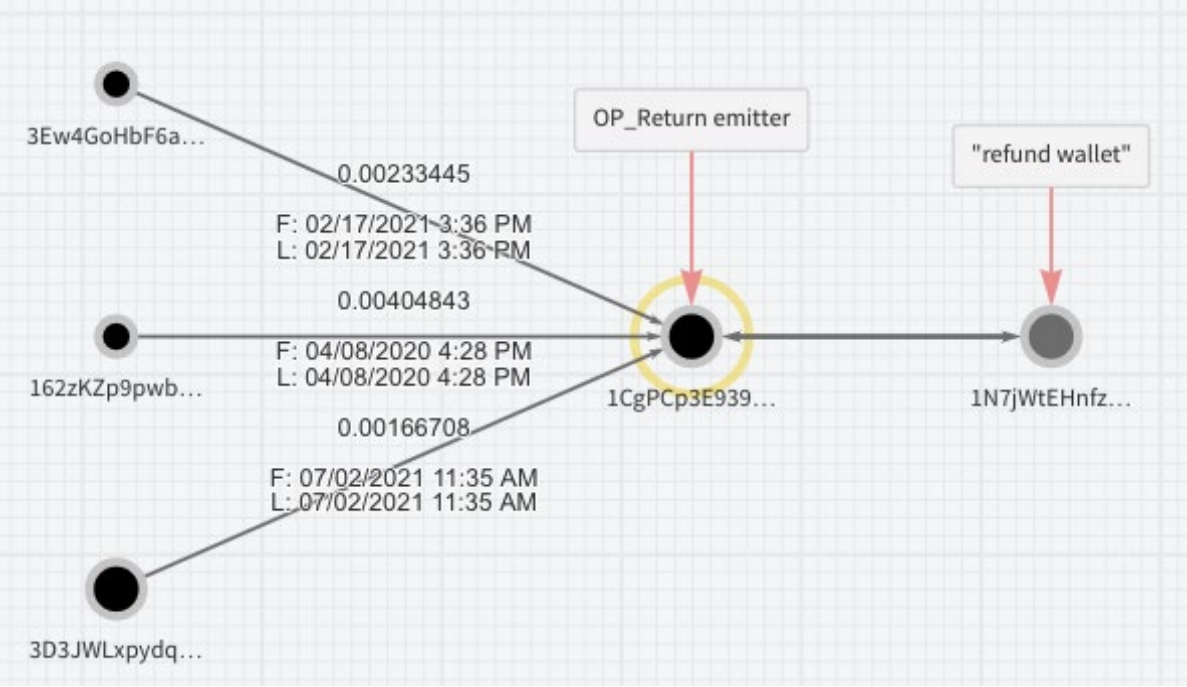
The last transaction occurring on May 13, 2020 still had the majority of funds unspent and unreturned to the 15y7d address.

Transactions from the 15y7d Address



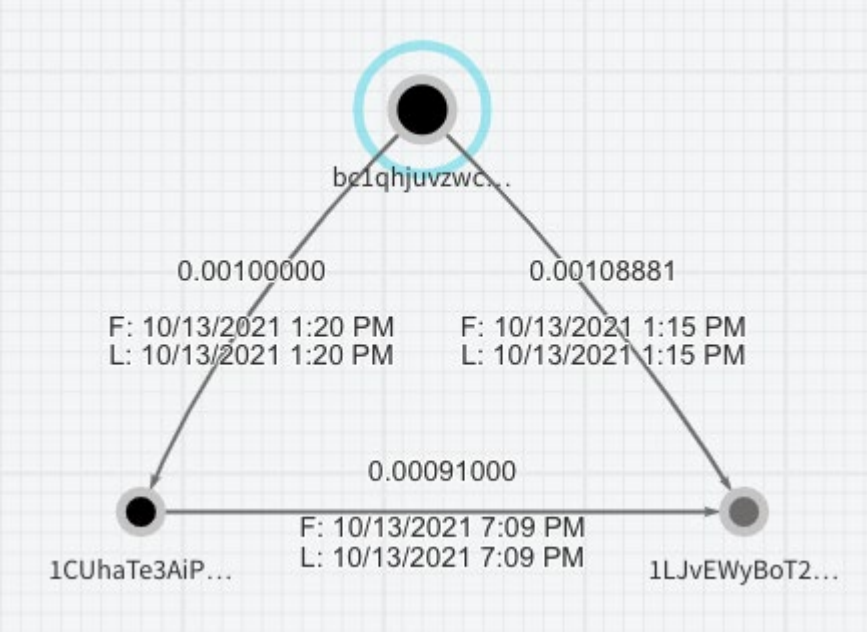
24. Chainalysis's blockchain analysis of the 1CgPC address shows a similar pattern of transactions. The 1CgPC address was active between April 8, 2020 and October 19, 2021. Chainalysis observed that the 1CgPC address's funds originated from transactions amounting to .00804996 Bitcoin sent from clusters identified by Chainalysis between February 17, 2021 and July 2, 2021. The 1CgPC address transactions were more efficient than the 15y7d address transactions, as they contained two outputs rather than three: the OP_Return and the Bitcoin address receiving the funds (1N7jWtEHnfz8MVV9raWY6Rfu6jLgCFZq2f). The funds received by the 1N7jW address generally were returned to the 1CgPC address on the same day.

Transactions from the 1CgPC Address



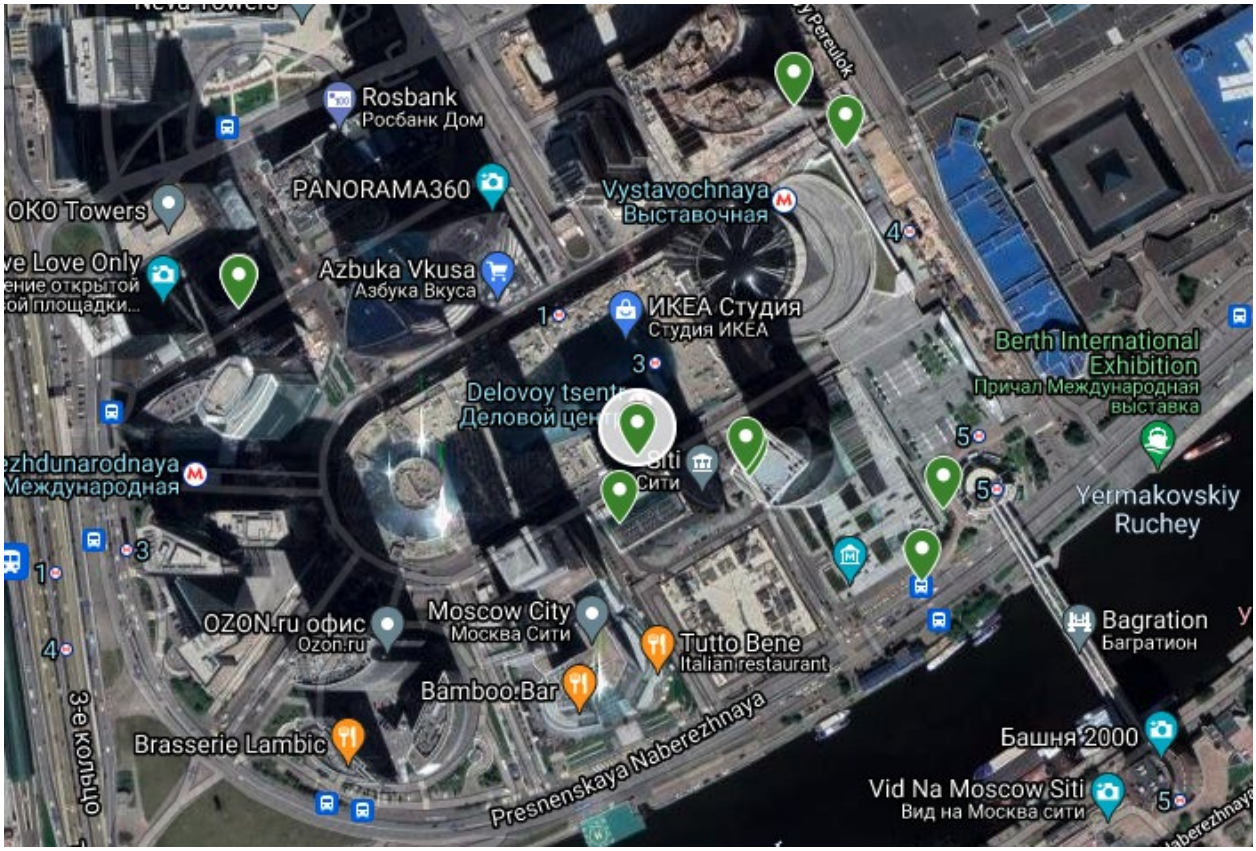
25. The 1CUha address was active on October 13, 2021. On this date, the 1CUha address was observed sending a small-value transfer to address 1LJvE,[7] with one accompanying OP_Return. The initial funding of the 1CUha address, also occurring on October 13, 2021, was observed coming from cluster bc1qhj,[8] which Chainalysis associated with Federation Tower, Presnenskaya emb., 12, Moscow, Russia, indicating that the entity in control of the wallet address likely conducted the transaction from the Federation Tower. The funding address also sent funds to address 1LJvE.

Transaction from the 1CUha Address



[7] The full address is 1LJvEWyBoT23vpCSmK5ooW6q2aPcutjXgk.
[8] The full address is bc1qhjuvzwcv0pp68kn2sqvx3d2k3pqfllv3c4vywd.

Location of cluster bc1qhj...



26. The transaction activity of the 15y7d, 1CgPC, and 1CUha addresses—intermittent and small-dollar transactions always with an OP_Return message—suggests that the Glupteba Enterprise is using the Bitcoin blockchain to send signals to the infected machines. Additionally, no OP_Return messages were observed being sent to the three hard-coded Glupteba Bitcoin addresses.

27. The OP_Returns were encrypted using a 256-bit Advanced Encryption Standard ("AES") specification. Using a decryption key hardcoded into Glupteba malware, the messages in OP_Returns can be decoded resulting in the following C2 server domains.

OP_Return Date	Address	Decrypted C2 Address
June 19, 2019, 06:10	15y7d	venoxcontrol.com
Jan. 24, 2020, 22:31	15y7d	robotatten.com
Feb. 14, 2020, 23:33	15y7d	sleepingcontrol.com
Feb. 17, 2020, 18:58	15y7d	anotheronedom.com
Mar. 28, 2020, 22:48	15y7d	getfixed.xyz
Mar. 28, 2020, 23:06	15y7d	gfixprice.xyz
Apr. 8, 2020, 17:24	1CgPC	sndvoices.com
May 7, 2020, 14:50	1CgPC	easywbdesign.com
May 13, 2020, 13:01	15y7d	maxbook.space
July 2, 2021, 10:33	1CgPC	evocterm.com
July 2, 2021, 10:50	1CgPC	evocterm.com
Feb. 17, 2021, 16:15	1CgPC	ninhaine.com
Oct. 13, 2021, 19:09	1CUha	tyturu.com
Oct. 19, 2021, 15:28	1CgPC	nisdably.com

28. As of October 25, 2021, there was a balance of 0.00675353 Bitcoin on the 1N7jW address which leads Chainalysis to believe with a high degree of certainty that funds are still pending to be returned to the 1CgPC address from transactions occurring with OP_Returns on February 18, 2021 and July 2, 2021. This is likely an indication that the C2 server domains in the OP_Return messages have not yet been utilized by the Glupteba botnet.

b. Other Findings

29. Google provided Chainalysis with metadata that Google's investigation found were associated with the Glupteba Enterprise. Chainalysis connected that

metadata to two Bitcoin clusters, the 173WD cluster and the bc1q04 cluster, in a manner that indicated that these clusters were controlled by a common entity.[9]

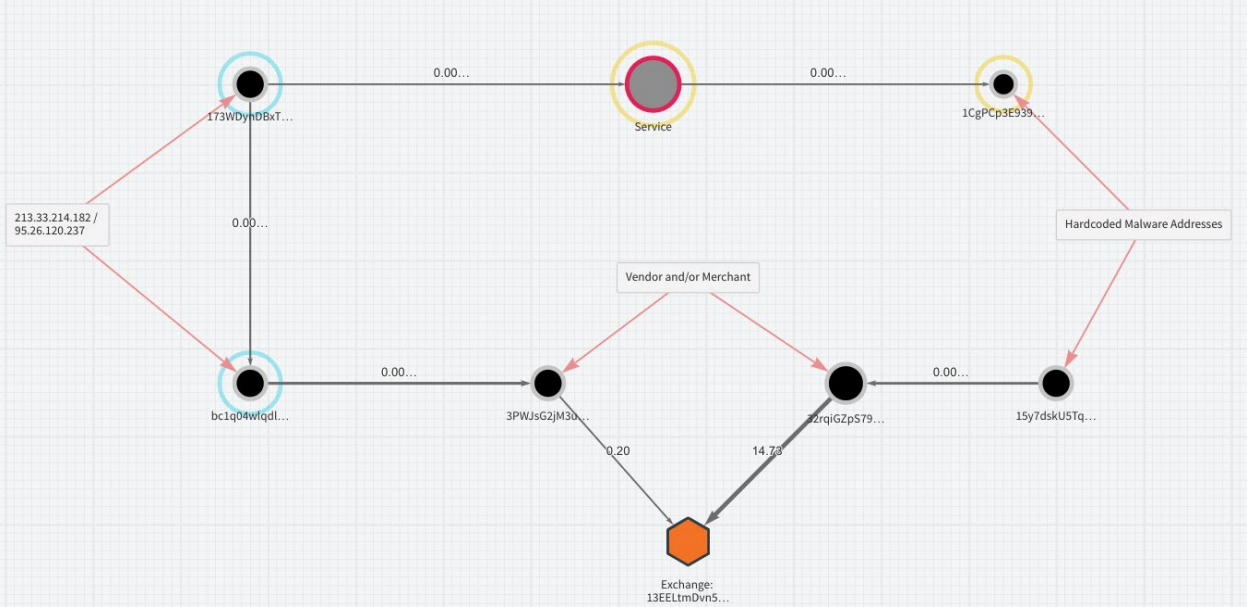
30. Chainalysis concluded based on its analysis of the blockchain that these two clusters likely belong to the same Bitcoin wallet. The 173WD cluster had two outputs to the bc1q04 cluster. The 173WD cluster made a deposit to a cluster that coincided with an output from the same cluster to the hard-coded Glupteba 1CgPC Bitcoin address, as shown below. This provides a clear connection from the 173WD cluster, and possibly the bc1q04 cluster, to the hard-coded Glupteba 1CgPC Bitcoin address.

31. On September 14, 2021, Chainalysis also found a Bitcoin address associated with AWMProxy.net: bc1qgst24xtn83cv0t8jkm49xjrwklfmry7egfn3qu (the "bc1qg address"). AWMProxy.net received a payment at this address. The bc1qg address has been observed transacting with an address associated with an exchange, known as a deposit address[10], which has only been used since June 2021 but has already accumulated over $1 million in Bitcoin. Chainalysis observed the bc1qg address receiving funds from the 173WD cluster, which, as previously stated, is strongly tied to the Bitcoin addresses hard-coded in the Glupteba malware to preserve its C2 server function. Chainalysis also observed additional funds deposited to the bc1qg address from known criminal markets, forums, and

[9] The full addresses are 173WDynDBxTt4zCG6FEK5x7wGLuXuHizto and bc1q04wlqdlus9ws9wqpfyyv3wnqd52s92qn7g0nzt, respectively.
[10] An exchange deposit address is an address typically associated with an individual's account held at an exchange, similar to an account held at a bank. The full address is bc1qeqmud3593upp5sem79nmgyl5ncsfqhxjm2wmw3.

ransomware proceeds, suggesting that AWMProxy.net services are used by various criminal operations.

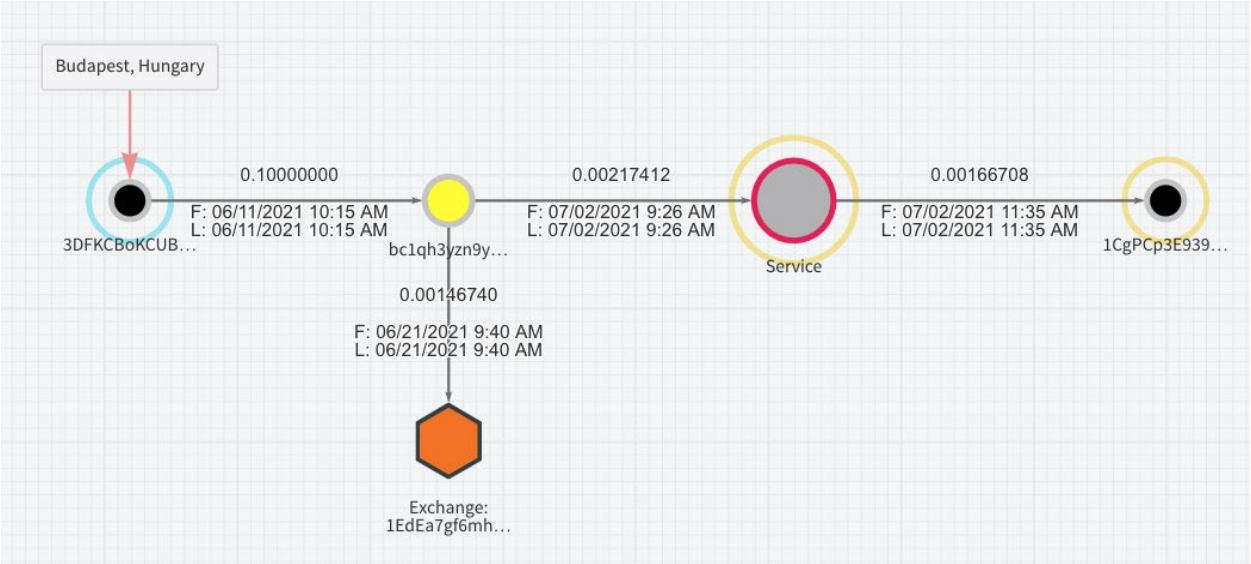
Activity of the 173WD Cluster



32. Chainalysis observed that another Bitcoin cluster—the bc1qh3 cluster[11]—made a deposit on July 2, 2021 to another cluster that coincided with a direct output to the hard-coded Glupteba Bitcoin 1CgPC address, as shown below. The origin of these funds was traced to Budapest, Hungary.

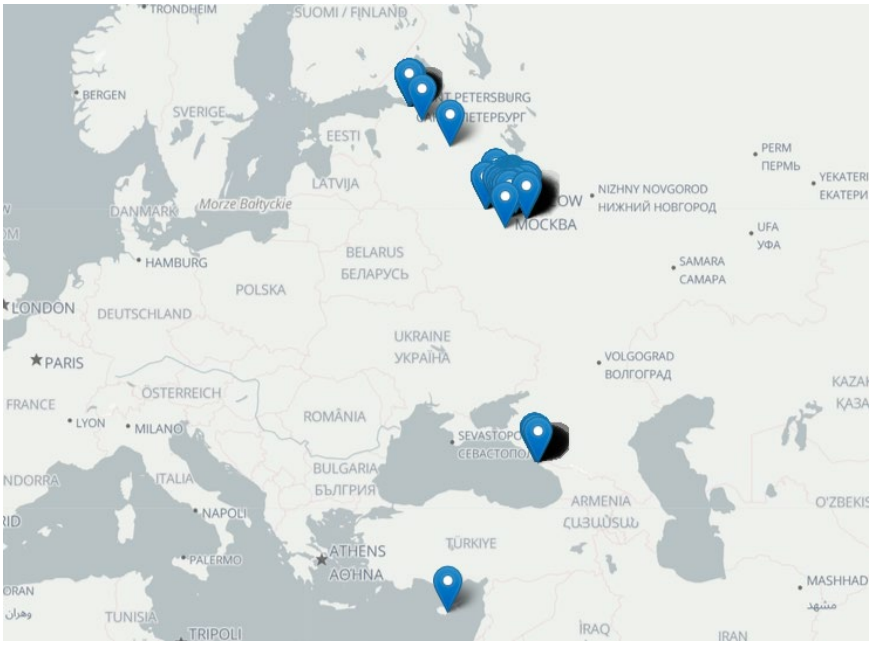
[11] The full address for this cluster is bc1qh3yzn9ywwx3840kprdmkngq8x86378zv96vwxt.

Activity of the bc1qh Cluster



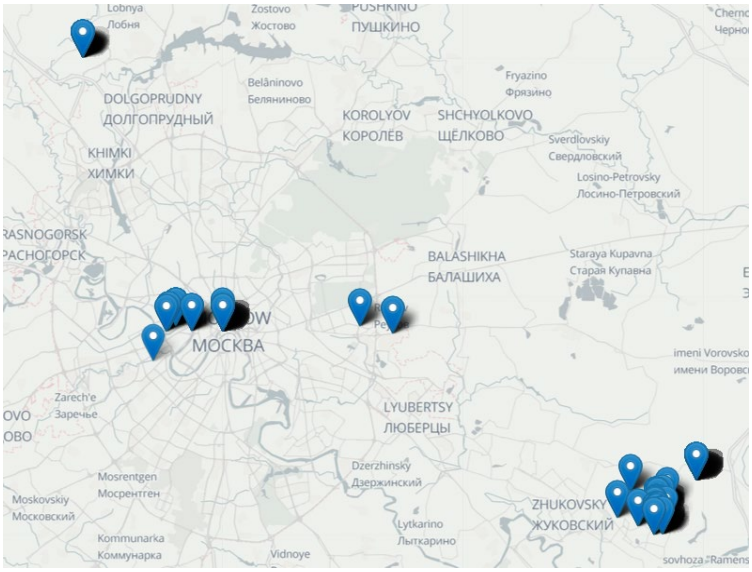
33. Chainalysis determined with a high degree of probability that the 173WD cluster was controlled by entities in and around Moscow, St. Petersburg, and Sochi, Russia, and the country of Cyprus, as shown below.

Location of 173WD Cluster IP Addresses



34. Chainalysis also determined with a high degree of probability that the bc1q04 cluster was controlled by entities in and around Moscow, Russia, as shown below.

Location of bc1q04 Cluster IP Addresses



35. Beyond the C2 server domains communicated through the OP_Return messages in Bitcoin transactions, there are domains used by the Glupteba malware, and hard-coded in the malware itself, that install payloads for a fee (Pay Per Install or PPI). Pay Per Install is used as a way to distribute malware; PPI typically starts with an affiliate building a network of infected computers while also earning money. The affiliate registers on a PPI site, like Install Capital, and receives a file from the PPI site provider. The affiliate binds the PPI files provided with another program that can then be hosted on the affiliate's site. When users then download the program from the affiliate's site, the malware gets installed on the user's computer. The affiliate is paid per user install of the malware issued from the PPI

site. Chainalysis observed domains hard-coded into recent samples of the malware in the following list:

Domain	Registrar	Sample SHA 256 Hash
iceanedy.com	Instra Corporation Pty Ltd.	e164923d190995c709d3d08f8d96825a7dbfdff4bf6b583dd4cc21b312f0d760
theatresearch.xyz	Namecheap	8ebe295051462bc139cd800d079ab2cad7598c92285a0913d65e482d99840643
okonewacon.com	DYNADOT, LLC	8ebe295051462bc139cd800d079ab2cad7598c92285a0913d65e482d99840643
blackempirebuild.com	Media Elite Holdings Limited	8ebe295051462bc139cd800d079ab2cad7598c92285a0913d65e482d99840643

36. Analysis conducted in September 2021 of past samples of the malware revealed additional domain names hard-coded in the malware. One related domain, gfixprice.space, is used to host samples and has a long history of submissions for files of the same name, which suggests that this could be a server hosting payloads for a PPI network. WHOIS registration data revealed the following about the registrant:

- Registrant Email: morkovskaya.v@gmail.com
- Registrant Phone: +380679485974
- Registrant Name: valentina morkovskaya

37. Finally, Chainalysis discovered that one of the physical addresses associated with Valtron[12] is Federation Tower, Presneskaya emb., 12, Moscow, Russia, the same address used by at least one other known criminal entity, Suex, a Czech-registered over-the-counter (OTC) exchange.

38. Between September 16, 2021 and September 24, 2021, Chainalysis researched Investavto LLC and found it was liquidated on September 23, 2021. During the same period, Chainalysis observed broader service disruptions of known Glupteba domains.[13]

39. Open-source intelligence, gathered by Google and Chainalysis, identified an employee review of Valtron LLC in which an individual indicates that Dont.farm is another name for Valtron LLC.

V. The Glupteba Enterprise's Illicit Cryptojacking Scheme

40. Chainalysis also validated with a high degree of probability public commentary that links the Glupteba Enterprise to the installation of PPI adware that uses the processing power of infected computers to mine cryptocurrency for the Enterprise. It is often impractical for a regular user of a personal computer to "mine" cryptocurrency due to the high electricity cost of running a computer with sufficient computing power for mining. The Glupteba Enterprise's cryptojacking scheme harnesses the combined power of numerous infected devices to mine

[12] Google identified Valtron or voltronwork.com as an entity associated with the Glupteba botnet's operations.
[13] Chainalysis observed disruptions to Trafspin.com, AWMProxy.net, and Abm.net on September 20, 2021.

cryptocurrencies. The Enterprise directs the rewards from the mining activity to its own cryptocurrency addresses, leaving the victims unaware that their computing power is contributing to a criminal enterprise that can be used by hackers or nation-states to generate illicit funds quickly and saddling them with being associated with illegal conduct, computing inefficiencies, and expenses.

In accordance with 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct. Executed on November 29, 2021, in Virginia.

Elizabeth Bisbee